Another case of violating privacy and personal data protection: Catt v. the United Kingdom

February 22, 2019 Guest Blogger Catt v the United Kingdom, Data protection, Right to Private Life

This blogpost was written by Judith Vermeulen, PhD researcher in the Law and Technology Research Group at Ghent University.

Shortly after *Big Brother Watch* (see also the blogpost for this case), the European Court of Human Rights again had the opportunity to pronounce itself on the compatibility of Article 8 ECHR with the collection, retention and further use of personal data for public interest purposes by UK authorities. *Catt*, however, does not involve an assessment of the data processing regime as such. Rather, it evaluates the specific situation the applicant is in. While the question of adequacy of the legal and regulatory framework surrounding the impugned measures remains unanswered, the processing of the applicant's data in particular is considered to not pass the necessity test. Noteworthy in any case is that the Court – in contrast to what the EU Court of Justice has decided in the past – reiterates that the indiscriminate collection of personal data is justifiable. With Brexit looming – and the CJEU accordingly soon losing its jurisdiction vis-à-vis Britain –, this development in the Strasbourg case-law is of particular importance. Finally, it is questionable whether Article 8 is in fact the best legal ground for assessing the facts of this case. The discussions these provoked at national may illustrate this point.

A history of protesting, a history of records

The applicant in this case is Mr John Oldroyd Catt, a British national born in 1925. Since 1948, when he joined the peace movement, he has been regularly attending public demonstrations. In March 2010, Mr. Catt requested, in accordance with section 7 of the UK's former 1998 Data Protection Act, access to information the police were holding on him. No less than sixty-six entries from nominal records for other individuals and information reports incidentally mentioning him, concerning incidents between March 2005 and October 2009, were disclosed to him. Fifty-three related to demonstrations organized by Smash EDO, whose object was to close down activities in the United Kingdom of EDO MBM Technology Ltd, a United States-owned company which manufactured weapons and weapon components and had a factory in Brighton, where the applicant lives. The Smash EDO protests, which the applicant began attending in 2005, attracted a substantial policing presence as they were associated with serious disorder and crime. There were additionally, another thirteen entries related to other, non-violent, gatherings. Thus, it was recorded that he had, amongst others, attended a Trades Union Congress Conference; had participated in a demonstration against "New Labour" organised by a number of trade unions; and had taken part in a pro-Gaza manifestation. The information included in the records were his name, presence, data of birth and address, sometimes a description of his appearance, and a photograph taken of him at an anti-Labour protest. His data were held in the National Special Branch Intelligence System, commonly referred to as the police's "Extremism database". When Mr. Catt subsequently asked the Association of Chief Police Officers ("ACPO") for their deletion, his request was declined without any further explanation.

From no interference at all to unjustified intrusion: disagreement at the domestic level

In March 2011, the applicant was granted permission to seek judicial review of the refusal. He claimed, more specifically, that the *retention* of his personal data was not "necessary" within the meaning of Article 8 ECHR. The domestic courts, in answering that question, all reached different conclusions.

On 31 October 2012, the High Court handed down its judgment in which it considered that Article 8 was not engaged in the case and that, even if it were, the interference was justified under Article 8, § 2 ECHR. In March 2014, the Court of Appeal, on the other hand, ruled that "[t]he systematic collection, processing and retention on a searchable database of personal information, even of relatively routine kind, involves a significant interference with the right to respect for private life". The interference can be justified "by showing that it serves the public interest in a sufficiently important way". In the Appeal Court's view, however, it was not shown that the information retained, over many years, which concerned Mr. Catt had in fact been of any assistance to the police at all and accordingly found the measure to be disproportionate. Almost exactly a year later, the Supreme Court, by four justices to one, upheld the appeal against the aforementioned judgment. While all five judges were of the opinion that Article 8 of the Convention was applicable, that both the *collection* and *retention* of the data amounted to a lawful interference with Mr. Catt's rights under that Article, and regarded the "necessity" criterion in relation to the *collection* to be fulfilled, only four found the latter also true regarding the *retention.*The majority took the view that the invasion of privacy involved in retaining information of this kind was minor in nature and extent, and concerned in no sense intimate or sensitive data. Rather, the information was about "the overt activities in public places of individuals whose main object in attending the events in question was to draw public attention to their support for a cause". They added bluntly that "[m]ost intelligence is necessarily acquired in the first instance indiscriminately": "[i]ts value can only be judged in hindsight, as subsequent analysis for particular purposes discloses a relevant pattern" and "[t]he most that can be done is to assess whether the value of the material is proportionate to the gravity of the threat to the public". As no nominal record was kept on the applicant, it was considered that the retention did not carry any stigma of suspicion or guilt. The fact that the material was not usable or disclosable other than for 'police purposes' was also deemed 'noteworthy'. The Supreme Court concluded that the material was periodically reviewed for retention or deletion according to rational and proportionate criteria, that sufficient safeguards existed to ensure that personal information was not retained for longer than required for the purpose of maintaining public order and preventing or detecting crime, and that disclosure to third parties was properly restricted. In his dissenting opinion, Lord Toulson, however, agreed with the Court of Appeal that the value of the applicant's data had not been evidenced. The suggestion that it would place too great a burden on the police to undertake frequent reviews he perceived as unconvincing.

In the meantime, an oversight report on undercover police operations designed to obtain intelligence about protest movements was published. As it found that information was unnecessarily being held in police records, it also triggered an extensive review operation of the police database covering overtly obtained intelligence. The number of reports mentioning the applicant was accordingly supposedly reduced from sixty-six to two. However, there appears to exist four additional and allegedly newly discovered records mentioning John Catt. They detail, amongst others, his presence at six separate events, not organised by Smash EDO. Five of them required a significant police operation, including arrests. With regard to the sixth no indication exists of whether that was the case also there.

A tempered violation in the eyes of Strasbourg

Before the European Court of Human Rights Mr. Catt complained that the *systematic collection* as well as the *retention* of information about him in a searchable database violated his Article 8 rights.

The Court, from its side, recalled that it is well-established in its case-law that even the mere *storing* of information – and consequently the *further processing* thereof – amounts to an interference with Article 8. It was fairly undisputed that the processing pursued the legitimate aim of preventing disorder or crime and safeguarding the rights and freedoms of others. As to whether the *collection*, *retention* and *use* of the applicant's personal data could be considered

“in accordance with the law”, it decided, in view of its conclusions in the negative in relation to the necessity thereof, that there was no need to answer that question definitely. Oddly enough the Court had, before coming to that conclusion, nonetheless extensively analysed the matter and identified a number of concerns.

Judge Koskelo, in her concurring opinion joined by Judge Felici, was nonetheless crystal clear on this point: “[t]he present case is […] essentially an individual manifestation of the consequences arising from shortcomings in the underlying legal framework”. The requirement of lawfulness indeed not only necessitates a measure to have a basis in domestic law. It also refers to the quality of the law in question: it should be adequately accessible and foreseeable as to it effects, and thus formulated with sufficient precision to enable any individual to regulate his conduct. At common law, and thus in the UK, the police have, however, a general – non-statutory – power to obtain and store information for policing purposes, including for the maintenance of public order and the prevention and detection of crime. Under those powers, and thus without any further legal basis thereto, the police have *collected* information relating to “domestic extremism”, which resulted in the creation of the abovementioned “Extremism database”. “Domestic extremism”, for which apparently exist three working definitions, was, for the purposes of the domestic proceedings, defined as “[…] the activity of individuals or groups who carry out criminal acts of direct action to further their protest, outside the democratic process”. As pointed out by Koskelo, “the records are held to help UK policing manage a future risk of crime”, “kept for policing purposes” and “include[…] information relating to extremism but also relating to public disorder that does not involve extremism”. The 2005 Code of Practice on the management of police information, adopted by the Secretary of State for the purpose of promoting the efficiency and effectiveness of police forces, limits the handling of police information to “policing purposes”, defined as “protecting life and property, preserving order, preventing crime, bringing offenders to justice and performing any legal duty or responsibility of the police”. In sum, the fundamental data protection principle of purpose limitation does not seem to have been respected, in neither phases of *collection* or *retention*. Thus, the purposes for processing, and thus the scope of the impugned measure in this case, are not clearly delineated and circumscribed in any regulatory instrument. As a consequence, individuals can indeed hardly be said to be enabled to foresee the consequences of their actions. Moreover, the effectiveness of any further characteristics of the *retention* and *use* regime depends largely on the definition of the purposes for processing. The Court found that those aspects were contained in the 1998 Data Protection Act and the 2005 Code of Practice. More specifically, data can be retained for a minimum of six years, after which the initial retention decision must be reviewed and the information accordingly may be deleted. These indeed do not change the fact that the police continues to have a general discretion to retain data if that is necessary for “policing”. As a result, they can potentially be *kept* and *used* indefinitely.

In analysing the lawfulness criterion, the Court, however, made a comparison with its judgment *in* M.M. v. the United Kingdom. In that case, the ECtHR did find a violation of Article 8 in view of the absence of clear and detailed statutory regulations governing, inter alia, the circumstances in which criminal record data could be collected, the duration of their storage, the use to which they could be put and the circumstances in which they may have been destroyed. While stating that the provisions on *retention* and *use* in *Catt* bear some similarity to those in *M.M.*, the Court in Strasbourg, in its analysis, nonetheless attached more weight to the differences between the facts of the two cases: the data retained would not be disclosed to third parties, and the applicant had the possibility to apply for deletion of his data. Hence, the ECtHR’s decision not to conclude whether or not the interference at hand could be considered “in accordance with the law”. The stated reasons are, however, in line with what the concurring judges stated, unpersuasive. The *disclosure* of personal data constitutes a separate interference with Article 8, must be thus justified in and of itself, and its absence cannot remedy a lack of safeguards in the phase of *collection* and *retention*. Furthermore, the fact that the applicant was able to, as well as actually requested, the disclosure and destruction of his data had a limited impact. The authorities refused the deletion and did not provide any

explanation for their continued retention. After the domestic proceedings, they, moreover, disclosed the retention of additional data without an explanation.

The “necessity” criterion, on the other hand was, as indicated above, not considered to be fulfilled. To come to this conclusion, the Court assessed whether a “pressing social need” existed for the interferences in dispute. The Court accepted that there existed a need to *collect* the personal data about the applicant. Thereto, the ECtHR, first of all, agreed with the Supreme Court that “it is in the nature of intelligence gathering that the police will first need to collect data, before evaluating its value”. With that, it reaffirmed its stance in *Big Brother Watch v. the United Kingdom* and contradicts the Court of Justice of the European Union: indiscriminate *collection* of personal data is justifiable and does not violate Article 8 ECHR. With Brexit coming up in just over a month, this development in the Strasbourg case-law may prove to be of significant value for the authorities in Britain. Secondly, it was pointed out that the personal data in question was overtly obtained. Although this argument was not further developed, it raises an important question: can *publicly available* personal data be granted protection under the right to respect for *private life* laid down in Article 8? Perhaps it may not. Indeed, as stated in the Supreme Court’s judgement, Mr. Catt’s main objective in attending the events in question was to draw public attention to his support for a cause. Unlike the EU Charter of Fundamental Rights, the European Convention does not foresee a separate right to protection of personal data which also covers information present in the public domain. Lastly, in finding that there was a “pressing social need” to collect the applicant’s data, the Court put forward that “[h]e had after all decided to repeatedly and publicly align himself with the activities of a violent protest group”.

Whether a pressing need to *retain* the applicant’s data existed, the majority, on the other hand, decided that there was not. Its main concern in that respect was that “in the absence of any rules setting a definitive maximum time limit on the retention of such data the applicant was entirely reliant on the diligent application of […] highly flexible safeguards […] to ensure the proportionate retention of his data”. Accordingly, in this context, the Court *did* point to the doubtful effectiveness of a number of those safeguards, being the data subjects’ right to access and right to object to the processing. The absence of effective safeguards was of particular concern as personal data revealing political opinions – “sensitive data” – attracts a heightened level of protection. In fact, it must – as the Court noted – have had a ‘chilling effect’ on the applicant’s right to engage in peaceful protest under Article 11 of the Convention, which also contains special protection for trade unions, whose events Mr Catt attended. Bearing in mind the observation made above concerning the fact that the applicant’s personal data may not ‘deserve’ protection under Article 8 of the Convention, an assessment of the facts of this case in the light of Article 11 instead would have been interesting, however, this did not occur in *Catt*. In its analysis, the Court further took into account the applicant’s age – he is roughly 93 years old. Finally, it dismissed the UK Government’s argument that it would be too burdensome to review the database and delete all the entries relating to the applicant. The acceptance of that contention would allow authorities to intentionally create databases in such a manner, and thus would allow for abuse.

The Court’s findings can be said to combine elements from both the UK’s Court of Appeal’s judgment and the Supreme Court’s. Indeed, the majority found that the potential eternal *retention* of the applicant’s data violates Article 8, while the indiscriminate *collection* of personal, especially overtly available, information does not. The decision, in any event, highlights the fact that the right to respect for private life as laid down in the ECHR, for the judges in Strasbourg, includes protection for non-private personal information. However, it could have been more convincing for the Court if Article 11 of the Convention, concerning the freedom of assembly and association, had been pushed as a more appropriate legal ground for evaluating the facts of this case.